

Bases for Vector Spaces

A set is **independent** if, roughly speaking, there is no redundancy in the set: You can't "build" any vector in the set as a linear combination of the others. A set **spans** if you can "build everything" in the vector space as linear combinations of vectors in the set. Putting these two ideas together, a **basis** is an independent spanning set: A set with no redundancy out of which you can "build everything".

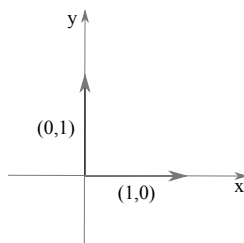
Definition. Let V be an F -vector space. A subset \mathcal{B} of V is a **basis** if it is linearly independent and spans V .

Definition. Let F be a field. The **standard basis** for F^n consists of the n vectors

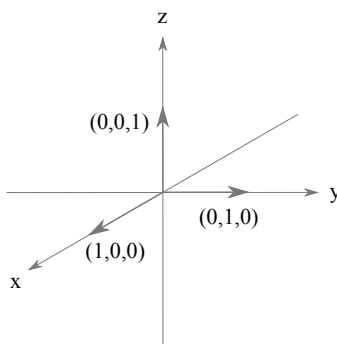
$$(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), (0, 0, 1, \dots, 0), \dots, (0, 0, 0, \dots, 1).$$

Thus, the k^{th} standard basis vector has a "1" in the k^{th} slot and zeros elsewhere.

The standard basis vectors in \mathbb{R}^2 are $(1, 0)$ and $(0, 1)$. They can be pictured as arrows of length 1 pointing along the positive x -axis and positive y -axis.



The standard basis vectors in \mathbb{R}^3 are $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$. They can be pictured as arrows of length 1 pointing along the positive x -axis, the positive y -axis, and the positive z -axis.



Since we're calling this a "basis", we'd better check that the name is justified!

Proposition. The standard basis is a basis for F^n .

Proof. First, we show that the standard basis spans F^n . Let $(a_1, a_2, a_3, \dots, a_n) \in F^n$. I must write this vector as a linear combination of the standard basis vectors. It's easy:

$$\begin{array}{r} a_1 \cdot (1, 0, 0, \dots, 0) \\ a_2 \cdot (0, 1, 0, \dots, 0) \\ a_3 \cdot (0, 0, 1, \dots, 0) \\ \vdots \\ + \quad a_n \cdot (0, 0, 0, \dots, 1) \\ \hline (a_1, a_2, a_3, \dots, a_n) \end{array}$$

For independence, suppose

$$a_1(1, 0, 0, \dots, 0) + a_2(0, 1, 0, \dots, 0) + a_3(0, 0, 1, \dots, 0) + \dots + a_n(0, 0, 0, \dots, 1) = (0, 0, 0, \dots, 0).$$

The computation we did to prove that the set spans shows that the left side is just $(a_1, a_2, a_3, \dots, a_n)$, so

$$(a_1, a_2, a_3, \dots, a_n) = (0, 0, 0, \dots, 0).$$

This implies that $a_1 = a_2 = a_3 = \dots = a_n = 0$, so the set is independent. \square

Aside from giving us an example of a basis for F^n , this result shows that at least one basis for F^n has n elements. We will show later that *every* basis for F^n has n elements.

Example. Prove that the following set is a basis for \mathbb{R}^3 over \mathbb{R} :

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$$

Make a matrix with the vectors as *columns* and row reduce:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Since A row reduces to the identity, it is invertible, and there are a number of conditions which are equivalent to A being invertible.

First, since A is invertible the following system has a unique solution for every (a, b, c) :

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

But this matrix equation can be written as

$$x \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + y \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + z \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

In other words, any vector $(a, b, c) \in \mathbb{R}^3$ can be written as a linear combination of the given vectors. This proves that the given vectors span \mathbb{R}^3 .

Second, since A is invertible, the following system has only $x = 0, y = 0, z = 0$ as a solution:

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

This matrix equation can be written as

$$x \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + y \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + z \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Since the only solution is $x = 0, y = 0, z = 0$, the vectors are independent.

Hence, the given set of vectors is a basis for \mathbb{R}^3 . \square

We'll generalize the computations we did in the last example.

Proposition. Let F be a field. $\{v_1, v_2, \dots, v_n\}$ is a basis for F^n if and only if

$$A = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \text{ is invertible. } \square$$

Remark. By earlier results on invertibility, this is equivalent to the following conditions:

1. A row reduces to the identity.
2. $\det A \neq 0$.
3. The system $Ax = 0$ has only $x = (x_1, x_2, \dots, x_n) = (0, 0, \dots, 0)$ as a solution.
4. For every vector $b = (b_1, b_2, \dots, b_n) \in F^n$, the system $Ax = b$ has a unique solution.

Thus, if you have n vectors in F^n , this gives you several ways of checking whether or not the set is a basis.

Proof. Suppose $\{v_1, v_2, \dots, v_n\}$ is a basis for F^n . Let

$$A = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix}.$$

Consider the system

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Doing the matrix multiplication on the left and writing the result as a vector equation, we have

$$x_1 v_1 + x_2 v_2 + \cdots + x_n v_n = (0, 0, \dots, 0).$$

Since $\{v_1, v_2, \dots, v_n\}$ is independent, I have $x_1 = x_2 = \cdots = x_n = 0$. This shows that the system above has only the zero vector as a solution. An earlier result on invertibility shows that A must be invertible.

Conversely, suppose the following matrix is invertible:

$$A = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix}.$$

We will show that $\{v_1, v_2, \dots, v_n\}$ is a basis.

For independence, suppose

$$x_1 v_1 + x_2 v_2 + \cdots + x_n v_n = (0, 0, \dots, 0).$$

Writing the left side as a matrix multiplication gives the system

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since A is invertible, the only solution to this system is $x_1 = x_2 = \cdots = x_n = 0$. This shows that $\{v_1, v_2, \dots, v_n\}$ is independent.

To show that $\{v_1, v_2, \dots, v_n\}$ spans, let $(b_1, b_2, \dots, b_n) \in F^n$. Consider the system

$$\begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Since A is invertible, this system has a (unique) solution (x_1, x_2, \dots, x_n) . That is,

$$x_1 v_1 + x_2 v_2 + \cdots + x_n v_n = (b_1, b_2, \dots, b_n).$$

This shows that $\{v_1, v_2, \dots, v_n\}$ spans.

Hence, $\{v_1, v_2, \dots, v_n\}$ is a basis for F^n . \square

A basis for V is a spanning set for V , so every vector in V can be written as a linear combination of basis elements. The next result says that such a linear combination is unique.

Proposition. Let \mathcal{B} be a basis for a vector space V . Every $v \in V$ can be written in exactly one way as

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n, \quad a_i \in F, \quad v_1, \dots, v_n \in \mathcal{B}.$$

Proof. Let $v \in V$. Since \mathcal{B} spans V , there are scalars a_1, a_2, \dots, a_n and vectors $v_1, \dots, v_n \in \mathcal{B}$ such that

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.$$

Suppose that there is another way to do this: There are scalars b_1, b_2, \dots, b_m and vectors $w_1, \dots, w_m \in \mathcal{B}$ such that

$$v = b_1 w_1 + b_2 w_2 + \cdots + b_m w_m.$$

First, note that I can assume that the same set of vectors are involved in both linear combinations — that is, the v 's and w 's are the same set of vectors. For if not, I can instead use the vectors in the union

$$S = \{v_1, \dots, v_n\} \cup \{w_1, \dots, w_m\}.$$

I can rewrite both of the original linear combinations as linear combinations of vectors in S , using 0 as the coefficient of any vector which doesn't occur in a given combination. Then both linear combinations for v use the same vectors.

I'll assume this has been done and just assume that $\{v_1, v_2, \dots, v_n\}$ is the set of vectors. Thus, I have two linear combinations

$$\begin{aligned} v &= a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \\ v &= b_1 v_1 + b_2 v_2 + \cdots + b_n v_n \end{aligned}$$

Then

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = b_1 v_1 + b_2 v_2 + \cdots + b_n v_n.$$

Hence,

$$(a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n = 0.$$

Since $\{v_1, v_2, \dots, v_n\}$ is independent,

$$a_1 - b_1 = 0, \quad a_2 - b_2 = 0, \dots, a_n - b_n = 0.$$

Therefore,

$$a_1 = b_1, \quad a_2 = b_2, \dots, a_n = b_n.$$

That is, the two linear combinations were actually the same. This proves that there's only one way to write v as a linear combination of vectors in \mathcal{B} . \square

I want to show that two bases for a vector space must have the same number of elements. I need some preliminary results, which are important in their own right.

Lemma. If A is an $m \times n$ matrix with $m < n$, the system $Ax = 0$ has nontrivial solutions.

Proof. Write

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

The condition $m < n$ means that the following system has more variables than equations:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

If A row reduces to a row reduced echelon matrix R , then R can have at most m leading coefficients. Therefore, some of the variables x_1, x_2, \dots, x_n will be free variables (parameters); if I assign nonzero values to the free variables (e.g. by setting all of them equal to 1), the resulting solution will be nontrivial. \square

Theorem. Let $\{v_1, v_2, \dots, v_n\}$ be a basis for a vector space V over a field F .

(a) Any subset of V with *more* than n elements is dependent.

(b) Any subset of V with *fewer* than n elements cannot span.

Proof. (a) Suppose $\{w_1, w_2, \dots, w_m\}$ is a subset of V , and that $m > n$. I want to show that $\{w_1, w_2, \dots, w_m\}$ is dependent.

Write each w as a linear combination of the v 's:

$$\begin{aligned} w_1 &= a_{11}v_1 + a_{12}v_2 + \cdots + a_{1n}v_n \\ w_2 &= a_{21}v_1 + a_{22}v_2 + \cdots + a_{2n}v_n \\ &\vdots \\ w_m &= a_{m1}v_1 + a_{m2}v_2 + \cdots + a_{mn}v_n \end{aligned}$$

This can be represented as the following matrix equation:

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ w_1 & w_2 & \cdots & w_m \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}.$$

Since $m > n$, the matrix of a 's has more columns than rows. Therefore, the following system has a nontrivial solution $x_1 = b_1, x_2 = b_2, \dots, x_m = b_m$:

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

That is, not all the b 's are 0, but

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

But then

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ w_1 & w_2 & \cdots & w_m \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

Therefore,

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ w_1 & w_2 & \cdots & w_m \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

In equation form,

$$b_1 w_1 + b_2 w_2 + \cdots + b_m w_m = 0.$$

This is a nontrivial linear combination of the w 's which adds up to 0, so the w 's are dependent.

(b) Suppose that $\{w_1, w_2, \dots, w_m\}$ is a set of vectors in V and $m < n$. I want to show that $\{w_1, w_2, \dots, w_m\}$ does not span V .

Suppose on the contrary that the w 's span V . Then each v can be written as a linear combination of the w 's:

$$\begin{aligned} v_1 &= a_{11}w_1 + a_{12}w_2 + \cdots + a_{1m}w_m \\ v_2 &= a_{21}w_1 + a_{22}w_2 + \cdots + a_{2m}w_m \\ &\vdots \\ v_n &= a_{n1}w_1 + a_{n2}w_2 + \cdots + a_{nm}w_m \end{aligned}$$

In matrix form, this is

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ w_1 & w_2 & \cdots & w_m \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix}.$$

Since $n > m$, the coefficient matrix has more columns than rows. Hence, the following system has a nontrivial solution $x_1 = b_1, x_2 = b_2, \dots, x_n = b_n$:

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Thus,

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Multiplying the v and w equation on the right by the b -vector gives

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ w_1 & w_2 & \cdots & w_m \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Hence,

$$\begin{bmatrix} \uparrow & \uparrow & \cdots & \uparrow \\ v_1 & v_2 & \cdots & v_n \\ \downarrow & \downarrow & \cdots & \downarrow \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

In equation form, this is

$$b_1v_1 + b_2v_2 + \cdots + b_nv_n = 0.$$

Since not all the b 's are 0, this is a nontrivial linear combination of the v 's which adds up to 0 — contradicting the independence of the v 's.

This contradiction means that the w 's *can't* span after all. \square

Corollary. Let F be a field.

- (a) Any subset of F^n with *more* than n elements is dependent.
- (b) Any subset of F^n with *fewer* than n elements cannot span.

Proof. This follows from the Theorem, and the fact that the standard basis for F^n has n elements. \square

As an example, the following set of *four* vectors in \mathbb{R}^3 can't be independent:

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ -3 \\ 10 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 11 \\ -7 \end{bmatrix} \right\}$$

Likewise, the following set of *two* vectors can't span \mathbb{R}^3 :

$$\left\{ \begin{bmatrix} -2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 5 \end{bmatrix} \right\} \quad \square$$

Corollary. If $\{v_1, \dots, v_n\}$ is a basis for a vector space V , then every basis for V has n elements.

Proof. If $\{w_1, \dots, w_m\}$ is another basis for V , then m can't be less than n or $\{w_1, \dots, w_m\}$ couldn't span. Likewise, m can't be greater than n or $\{w_1, \dots, w_m\}$ couldn't be independent. Therefore, $m = n$. \square

The Corollary allows us to define the **dimension** of a vector space.

Definition. The number of elements in a basis for V is called the **dimension** of V , and is denoted $\dim V$.

The definition makes sense, since in a finite-dimensional vector space, any two bases have the same number of elements. This is true in general; I'll state the relevant results without proof.

- (a) Every vector space has a basis. The proof requires a set-theoretic result called **Zorn's Lemma**.

(b) Two bases for *any* vector space have the same **cardinality**. Specifically, if \mathcal{B} and \mathcal{C} are bases for a vector space V , there is a bijective function $f: \mathcal{B} \rightarrow \mathcal{C}$.

Here's an example of a basis with an infinite number of elements.

Example. Let $\mathbb{R}[x]$ denote the \mathbb{R} -vector space of polynomials with coefficients in \mathbb{R} .

Show that $\{1, x, x^2, x^3, \dots\}$ is a basis for $\mathbb{R}[x]$.

First, a polynomial has the form $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. This is a linear combination of elements of $\{1, x, x^2, x^3, \dots\}$. Hence, the set spans $\mathbb{R}[x]$.

To show that the set is independent, suppose there are numbers $a_0, a_1, \dots, a_n \in \mathbb{R}$ such that

$$a_0 + a_1 x + \dots + a_n x^n = 0.$$

This equation is an *identity* — it's true for all $x \in \mathbb{R}$. Setting $x = 0$, I get $a_0 = 0$. Then plugging $a_0 = 0$ back in gives

$$a_1 x + \dots + a_n x^n = 0.$$

Since this is an identity, I can differentiate both sides to obtain

$$a_1 + 2a_2 x + \dots + na_n x^{n-1} = 0.$$

Setting $x = 0$ gives $a_1 = 0$. Plugging $a_1 = 0$ back in gives

$$2a_2 x + \dots + na_n x^{n-1} = 0.$$

Continuing in this way, I get $a_0 = a_1 = \dots = a_n = 0$. Hence, the set is independent.

Therefore, $\{1, x, x^2, x^3, \dots\}$ is a basis for $\mathbb{R}[x]$. \square

The next result shows that, in principle, you can construct a basis by:

- (a) Starting with an independent set and adding vectors.
- (b) Starting with a spanning set and removing vectors.

Theorem. Let V be a finite-dimensional vector space.

- (a) Any set of independent vectors is a subset of a basis for V .
- (b) Any spanning set for V contains a subset which is a basis.

Part (a) means that if S is an independent set, then there is a basis T such that $S \subset T$. (If S was a basis to begin with, then $S = T$.) Part (b) means that if S is a spanning set, then there is a basis T such that $T \subset S$.

I'm only proving the result in the case where V has finite dimension n , but it is true for vector spaces of any dimension.

Proof.

(a) Let $\{v_1, \dots, v_m\}$ be independent. If this set spans V , it's a basis, and I'm done. Otherwise, there is a vector $v \in V$ which is not in the span of $\{v_1, \dots, v_m\}$.

I claim that $\{v, v_1, \dots, v_m\}$ is independent. Suppose

$$av + a_1 v_1 + \dots + a_m v_m = 0.$$

Suppose $a \neq 0$. Then I can write

$$v = -\frac{1}{a}(a_1 v_1 + \dots + a_m v_m).$$

Since v has been expressed as a linear combination of the v_k 's, it's in the span of the v_k 's, contrary to assumption. Therefore, this case is ruled out.

The only other possibility is $a = 0$. Then $a_1v_1 + \cdots + a_mv_m = 0$, so independence of the v_k 's implies $a_1 = \cdots = a_m = 0$. Therefore, $\{v, v_1, \dots, v_m\}$ is independent.

I can continue adding vectors in this way until I get a set which is independent and spans — a basis. The process must terminate, since no independent set in V can have more than n elements.

(b) Suppose $\{v_1, \dots, v_m\}$ spans V . I want to show that some subset of $\{v_1, \dots, v_m\}$ is a basis.

If $\{v_1, \dots, v_m\}$ is independent, it's a basis, and I'm done. Otherwise, there is a nontrivial linear combination

$$a_1v_1 + \cdots + a_mv_m = 0.$$

Assume without loss of generality that $a_1 \neq 0$. Then

$$v_1 = -\frac{1}{a_1}(a_2v_2 + \cdots + a_mv_m).$$

Since v_1 is a linear combination of the other v 's, I can remove it and still have a set which spans V ; that is, $V = \langle v_2, \dots, v_m \rangle$.

I continue throwing out vectors in this way until I reach a set which spans and is independent — a basis. The process must terminate, because no set containing fewer than n vectors can span V . \square

It's possible to carry out the “adding vectors” and “removing vectors” procedures in some specific cases. The algorithms are related to those for finding bases for the **row space** and **column space** of a matrix, which I'll discuss later.

Suppose you know a basis should have n elements, and you have a set S with n elements (“the right number”). To show S is a basis, you only need to check *either* that it is independent *or* that it spans — not both. I'll justify this statement, then show by example how you can use it. I need a preliminary result.

Proposition. Let V be a finite dimensional vector space over a field F , and let W be a subspace of V . If $\dim W = \dim V$, then $V = W$.

Proof. Suppose $\dim W = \dim V = n$, but $V \neq W$. I'll show that this leads to a contradiction.

Let $\{x_1, x_2, \dots, x_n\}$ be a basis for W . Suppose this is not a basis for V . Since it's an independent set, the previous result shows that I can add vectors y_1, y_2, \dots, y_m to make a basis for V :

$$\{x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m\}.$$

But this is a basis for V with more than n elements, which is impossible.

Therefore, $\{x_1, x_2, \dots, x_n\}$ is also a basis for V . Let $x \in V$. Since $\{x_1, x_2, \dots, x_n\}$ spans V , I can write x as a linear combination of the elements of $\{x_1, x_2, \dots, x_n\}$:

$$x = a_1x_1 + a_2x_2 + \cdots + a_nx_n, \quad a_i \in F.$$

But since x_1, x_2, \dots, x_n are in W and W is a subspace, any linear combination of x_1, x_2, \dots, x_n must be in W . Thus, $x \in W$.

Since x was an arbitrary element of V , I get $V \subset W$, so $W = V$. \square

You might be thinking that this result is obvious: W and V have the same dimension, and you can't have one thing inside another, with both things having the “same size”, unless the things are equal. This is intuitively what is going on here, but this kind of intuitive reasoning doesn't always work. For example, the even integers are a subset of the integers and, as infinite sets, both are of the same “order of infinity” (**cardinality**). But the even integers aren't all of the integers: There are odd integers as well.

Corollary. Let S be a set of n vectors in an n -dimensional vector space V .

(a) If S is independent, then S is a basis for V .

(b) If S spans V , then S is a basis for V .

Proof. (a) Suppose S is independent. Consider W , the span of S . Then S is independent and spans W , so S is a basis for W . Since S has n elements, $\dim W = n$. But $W \subset V$ and $\dim V = n$. By the preceding result, $V = W$.

Hence, S spans V , and S is a basis for V .

(b) Suppose S spans V . Suppose S is not independent. By an earlier result, I can remove some elements of S to get a set T which is a basis for V . But now I have a basis T for V with fewer than n elements (since I removed elements from S , which had n elements).

This is a contradiction, and hence S must be independent. \square

Example. (a) Determine whether $\{(1, 2, 1), (2, 1, 1), (2, 0, 1)\}$ is a basis for the \mathbb{Z}_3 vector space \mathbb{Z}_3^3 .

(b) Determine whether $\{(1, 1, 0), (1, 2, 2), (2, 2, 0)\}$ is a basis for the \mathbb{Z}_3 vector space \mathbb{Z}_3^3 .

(a) Form the matrix with the vectors as columns and row reduce:

$$\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Since the matrix row reduces to the identity, it is invertible. Since the matrix is invertible, the vectors are independent. Since we have 3 vectors in a 3-dimensional vector space, the Corollary says that the set is a basis. \square

(b) Form the matrix with the vectors as columns and row reduce:

$$\begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 2 \\ 0 & 2 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The matrix did not row reduce to the identity, so it is not invertible. Since the matrix is not invertible, the vectors aren't independent. Hence, the vectors are not a basis. \square